UNITED STATES OF AMERICA
BEFORE THE
DEPARTMENT OF ENERGY

Securing the United States Bulk-Power System	)))	Docket No. DOE–HQ–2020–0028

COMMENTS OF THE ISO-RTO COUNCIL

The ISO-RTO Council ("IRC")[1] submits these comments and responses in reply to the United States Department of Energy's ("DOE") Notice of Request for Information ("RFI") published in the Federal Register on July 8, 2020, in the above-captioned proceeding. In the RFI, the DOE seeks information to understand the energy industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system ("BPS").

I. BACKGROUND

The IRC supports the goal outlined in the President's Executive Order 13920 ("E.O. 13920"), issued May 1, 2020, to address supply chain risks associated with physical assets, control systems, and software associated with actions of foreign adversaries. The electric industry is already subject to mandatory cybersecurity standards required by Congress through the Energy Policy Act of 2005.[2] Consistent with these requirements, the industry

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"), California Independent System Operator ("CAISO"), Electric Reliability Council of Texas, Inc. ("ERCOT"), the Independent Electricity System Operator of Ontario, Inc. ("IESO"), ISO New England Inc. ("ISO-NE"), Midcontinent Independent System Operator, Inc. ("MISO"), New York Independent System Operator, Inc. ("NYISO"), PJM Interconnection, L.L.C. ("PJM"), and Southwest Power Pool, Inc. ("SPP").

[2] The Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005) ("EPAct 2005").

worked collectively through the North American Electric Reliability Corporation ("NERC") standards development and stakeholder process to present to the Federal Energy Regulatory Commission ("FERC") the CIP-005-6, CIP-010-3, and CIP-013-1 Critical Infrastructure Protection ("CIP") standards (collectively, the "Cybersecurity Supply Chain Risk Management Standards").

The CIP Supply Chain Cybersecurity Risk Management Standards are intended to be forward-looking, risk-based standards for entities to mitigate cyber security risks to the reliable operation of the Bulk Electric System ("BES"). Under the standards, each responsible entity is required to develop and implement security controls as part of the entity's overall supply chain risk management documented plans. These plans focus on software integrity and authenticity, vendor remote access to BES cyber systems, information system planning, and risk management and procurement controls for purchasing software, hardware, and services from vendors.

Although the industry has worked to address supply chain risk issues through these standards, the industry is largely a purchaser of equipment, hardware, and software, and, therefore, an 'end user' in the supply chain. Use of Presidential authority to reach higher up the chain to vendors and suppliers of the equipment needed by the industry is a key link to ensuring that supply chain controls are adequate from one end of the supply chain to the other.

II. COMMENTS

Many of the questions raised in the RFI relate directly to the sale and purchase of physical assets such as generators and substation apparatus. ISOs and RTOs are bulk electric system operators that do not own or manage such physical assets but do own and

manage the software and systems needed to manage the grid. For this reason, the IRC is not the best entity to answer most of the questions posed by the RFI. While the IRC does provide responses to some of the RFI's questions in the attached appendix, the IRC's primary purpose in these comments is to underscore certain key principles that the DOE should consider in implementing the Executive Order.

A. Defining the Scope of the Executive Order's Application

The breadth of E.O. 13920 is quite sweeping, encompassing all equipment used in the BPS. While the IRC agrees with the general direction of the order, the IRC is concerned that prohibiting any transaction involving equipment with one or more components manufactured by companies with links to countries preliminarily identified as "foreign adversaries" could itself pose a reliability risk to the BPS. The IRC understands that the vast majority of BPS equipment includes at least some components manufactured by Chinese companies or companies with operations in China. In the event new equipment is needed to replace failed equipment or to meet new load growth or other transmission system needs, it is possible that no compliant equipment would be available to an affected utility. For this reason, the DOE should apply some reasonable limit on the scope of the order—at least until manufacturers throughout the supply chain can begin developing components and equipment that would enable compliance with a broader application of the order.

To this end, the IRC recommends that the DOE conduct a risk assessment based on the equipment's relative impact on grid reliability and the difficulty of replacement, among other factors. Equipment that has broader grid impacts or that affects critical customers or functions should be prioritized over equipment that impacts only a small part of the BPS

or that impairs less critical functions. On the other hand, the reliability risk associated with the difficulty of replacing certain equipment under the Executive Order's more constrained supply regime should also be considered. Grid impacts due to loss of control must be appropriately balanced with recovery and replacement impacts so that the most critical equipment can be replaced with as little disruption to system reliability as is possible. This is a complex modeling exercise, which will require not just the resources of the National Labs but also the input from the industry through communication with the Electric Sector Coordinating Council ("ESCC") and discrete industry segments and vendors.

For these reasons, the IRC urges the DOE to work with the ESCC as the primary vehicle (along with vendors and representative organizations such as the IRC) to create a clear plan to focus these efforts.[3]

B. Clear Guidance for the Interim Period

The IRC recommends that DOE consider providing clear guidance to the industry for procuring equipment during the period before the rules implementing the order are finalized and implemented. Although the DOE has in its various presentations indicated its intent to focus on the greatest risks, industry executives could still be reluctant to make major investments, fearing prudence challenges from regulators or shareholders concerning necessary replacements or upgrades of equipment they have taken during this interim period before the final DOE rules have been promulgated. For this reason, the IRC also recommends the DOE work with the ESCC along with vendors and industry

[3] Such efforts should also account for the fact that the list of foreign nations that pose a threat to energy supply chains may change over time and may require periodic reprioritization.

organizations such as the IRC to develop clear guidance to the industry as to how to proceed during the interim period while a plan is being both developed and executed.

C. Security of Information

In moving forward with this effort, it is important to establish a means to protect the security of the information that the industry is being asked to provide through the RFI and through related efforts as part of implementation of the E.O. 13920. Although Congress through the Fixing America's Surface Transportation Act ("FAST Act")[4] provided the DOE additional tools to safeguard such information, there remain legal challenges by persons seeking the public release of such information. Without adequate protection, the industry will be loath to share information concerning its most vulnerable equipment.

Reducing supply chain risks also requires transparency into supply chain risks that can only be provided by the Federal government. Providing mechanisms for greater transparency and security of that information will be important. The use of clearances should be considered to help provide greater information sharing and security of government intelligence related to supply chain threats.

By the same token, the electric industry today involves many more players, many of whom are often competitors of each other. Steps will need to be taken to ensure protection against disclosure of competitively sensitive information and antitrust protection for the sharing of vulnerabilities in equipment that will be necessary to ensure that the best information is gathered and effective industry-wide solutions are developed. The IRC stands ready to work with DOE on this effort.

[4] *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94.

III. ANSWERS TO QUESTIONS POSED IN THE REQUEST FOR INFORMATION

In the appendix to these comments, the IRC provides responses to some of the more pertinent DOE questions that relate to the role of RTOs and ISOs in supply chain risk management.

IV. CONCLUSION

The IRC is an active member of the ESCC and its various work groups. The IRC stands ready to work with the DOE on this important effort both through the ESCC as well as individually. We look forward to continuing dialogue and work with DOE on this important task.

Respectfully submitted,

/s/ Tyler E. Barnett
Maria Gulluni
Vice President & General Counsel
Tyler E. Barnett
Corporate Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
tbarnett@iso-ne.com

/s/ Craig Glazer
Craig Glazer
Vice President-Federal Government Policy
James M. Burlew
Senior Counsel
PJM Interconnection, L.L.C.
2750 Monroe Boulevard
Audubon, Pennsylvania 19403
james.burlew@pjm.com

/s/ Anna McKenna
Roger E. Collanton, General Counsel
Anna McKenna
Assistant General Counsel, Regulatory
Andrew Ulmer Director, Federal Regulatory Affairs
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
amckenna@caiso.com

/s/ Christopher R. Sharp
Robert E. Fernandez, General Counsel
Raymond Stalter
Director of Regulatory Affairs
Carl F. Patka
Assistant General Counsel
Christopher R. Sharp
Senior Compliance Attorney
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144

cpatka@nyiso.com

/s/ Andre T. Porter
Andre T. Porter
Vice President, General Counsel & Secretary
Mary-James Young
Senior Corporate Counsel
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
aporter@misoenergy.org

/s/ Paul Suskie
Paul Suskie
Executive Vice President & General Counsel
Mike Riley
Associate General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Devon Huber
Devon Huber
Senior Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto Ontario M5H1T1
Canada
devon.huber@ieso.ca

/s/ Chad V. Seely
Chad V. Seely
Vice President and General Counsel
Nathan Bigbee
Assistant General Counsel
Brandon Gleason
Senior Corporate Counsel
Electric Reliability Council of Texas, Inc.
7620 Metro Center Drive
Austin, Texas 78744
chad.seely@ercot.com

/s/ Diana Wilson
Diana Wilson
Director Enterprise Risk Management and Compliance
Alberta Electric System Operator
#2500, 330 — 5 Avenue SW
Calgary, Alberta T2P 0L4
Diana.wilson@aeso.ca

August 24, 2020

Appendix

IRC Responses to
RFI Questions Applicable to IRC Members

In response to the certain questions posed by the DOE in the RFI, the IRC provides the following.[5]

A. Responses to Questions in No. A–5

1. What governance of sub-tier vendors do energy sector asset owners and/or vendors have in place?

There is currently no regulatory requirement for governance of sub-tier vendors for energy sector asset owners. NERC Reliability Standard CIP-013 requires asset owners to govern the supplier, but not sub-tier suppliers. As a result, the level of depth of suppliers that asset owners include in their supply chain programs is at their own discretion, based on risk.

2. Is contract language for Supply Chain Security included in procurement contracts?

Energy sector asset owners are required to meet certain requirements in the pre-purchasing and purchasing phases of hardware and software supporting BES Cyber Systems. The implementation of these requirements is generally by proposing language in procurement contracts. Asset owners cannot force a vendor to accept the terms required to be proposed.

3. Are metrics for supply chain security, along with cost, schedule, and performance maintained?

Metrics associated with supply chain cybersecurity are tracked at the discretion of each energy sector asset owner.

[5] The IRC responds to only certain questions in the Request for Supplemental Comments because many of the questions in the Request for Supplemental Comments are technical questions that are better addressed by electric storage resources, small generators, and their manufacturers.

B. Responses to Questions in No. A–6

1. Can energy sector asset owners and/or vendors document the level of engagement in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise (e.g., Information Sharing and Analysis Center, Information Sharing and Analysis Organization)?

Members of the ISO/RTO community have been actively involved with the DOE in supply chain threat information sharing and development of best practices for testing. In addition, the ISOs/RTOs participate in information sharing with other organizations as described below.

2. Does the energy sector participate in a community for sharing supply chain risks?

Energy sector asset owners do not currently have formally defined programs for sharing supply chain threats and vulnerabilities. Many asset owners rely upon alerts published by the US Department of Homeland Security through the US-CERT and ICS-CERT to be alerted about important vulnerabilities. The ISOs/RTOs are actively involved with the North American Transmission Forum in developing best practices among industry, vendors, and assessors to mitigate supply chain threats.

Informal communication occurs between asset owners in various industry stakeholder groups and, in some cases, in classified government briefings. Energy sector asset owners maintain regular communication with the E-ISAC regarding events and incidents, but this is not typically focused on supply chain.

3. Does the energy sector encourage security related information exchange with external entities, including the Federal government?

Energy sector asset owners are encouraged to exchange information with a variety of Federal government entities. This includes federal agencies in both the United States

and Canada. In most cases, energy asset owners depend upon the Federal government to share supply chain threats, since asset owners do not have direct visibility to nation-state threats in supply chains. Asset owners also rely on open source information and commercial sources from security vendors.

C. Responses to Questions in No. A–7

1. What physical and logistical role-based access control policies have been developed to monitor and restrict access during installation when a foreign adversary, or associated foreign owned, foreign-controlled, or foreign influenced person is installing BPS electric equipment at a BPS site in the U.S.?

ISOs/RTOs utilize proper screening and assurance of security controls to restrict access to suppliers, installers, integrators, or service providers. . NERC Reliability Standard CIP-004 requires access control for all personnel who require physical or logical access to BPS equipment. This includes background checks, approval of access, and periodic recertification and reconciliation of access. NERC Reliability Standard CIP-006 requires specific security processes for physical access to BPS sites. NERC CIP requirements subject to future enforcement will also require asset owners to identify and be able to terminate remote vendor access sessions.

2. What policies and practices exist to ensure installers/integrators effectively protect the systems and components during installation and commissioning?

Asset owners monitor logical access using security event monitoring processes, as defined in NERC Reliability Standard CIP-007, to detect possible violations of cyber access. Physical security event monitoring processes, as defined in NERC Reliability Standard CIP-006, are also required to monitor on-site work. Logical system configuration is also monitored to ensure security controls are in place through configuration

management, vulnerability assessment, and test procedures, as required by the NERC CIP Reliability Standards.

3. What policies and practices are in place to ensure that service providers (including those providing remote monitoring and management of systems) effectively maintain the security protections of the systems and components they are monitoring?

See previous answer, which addresses the security requirements for installers and integrators.

4. Does an insider threat program exist?

Formally defined insider threat programs are not currently required for asset owners, but many asset owners have developed such programs. These programs generally include alignment with best practices, coordination between business units, detection and monitoring processes and technologies, as well as incident response processes.

D. Responses to Questions in No. B–2

1. Within the E.O. 13920 definition of BPS electric equipment, are there categories of BPS electric equipment that are more reliant on vendors likely to become the subject of transaction reviews, and if so, what are they? What are the sourcing challenges and cost impacts for companies facing prohibited transactions for those BPS electric equipment categories?

Systems and equipment used by ISOs/RTOs are designed, developed, and integrated over decades. Changes require careful coordination with transmission owners and operators in a given control area. As a result, any changes in ISO/RTO supply chains as a result of transaction reviews will be challenging, costly, and will take time to mitigate. The number of vendors that provide products and services to ISOs/RTOs is limited, and the foreign nations involved have not typically been considered threats to the US. At the

same time, there is limited ability to assess supply chain threats at the sub-tier level for these vendors.